Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Артеменков Михаил Николаевич
Должность: Ректор
Дата подписания: 09.11.2026 17:44:33
Уникальный программный ключ:
a63b74166e8f4fc17bd1e0462725f79e393bfdf9

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

Кафедра аналитических и цифровых технологий

«УТВЕРЖДАЮ»
Проректор по учебно-
методической работе
_____ Ю.А. Устименко
«30» июня 2022 г.

Рабочая программа дисциплины
Б1.О.06 Информационная безопасность компании

Направление подготовки 38.04.01 Экономика
Направленность (профиль): Финансовая безопасность и контроллинг
Форма обучения – заочная
Курс – 1
Семестр – 1
Всего зачетных единиц – 5, часов – 180
Форма отчетности: зачет – 1 семестр

Программу разработал:
кандидат физико-математических наук, доцент Букачев Д.С.

Одобрена на заседании кафедры аналитических и цифровых технологий
«23» июня 2022 года, протокол № 10

Заведующий кафедрой _____ Д.С. Букачев

Смоленск
2022

1. Место дисциплины в структуре ОП

Дисциплина «Информационной безопасности» является обязательной дисциплиной вариационной части образовательной программы по направлению подготовки 38.03.01 Экономика.

Изучение дисциплины предполагает сочетание фундаментальной подготовки с освоением технологии применения специализированных программных продуктов и систем, ориентированных на защиту экономической и служебной информации, служит базисом для формирования компетенций, сформированных при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений, таких, как «Современные информационно-коммуникационные технологии в научных исследованиях», «Компьютерные технологии в учёте и налогообложении», «Учебно-тренинговый комплекс "1С бухгалтерия"», «Интеллектуальные информационные системы в экономике».

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Компетенция	Индикаторы достижения *(в соответствии с разделом 6 общей характеристики ОП ВО)*
ОПК-4 Способен принимать экономически и финансово обоснованные организационно-управленческие решения в профессиональной деятельности и нести за них ответственность	**Знать**: методы принимать экономически и финансово обоснованные организационно-управленческие решения в профессиональной деятельности и нести за них ответственность для целей экономической безопасности в экономическом и правовом аспекте; основные риски информационной безопасности. **Уметь**: принимать экономически и финансово обоснованные организационно-управленческие решения в профессиональной деятельности и нести за них ответственность в целях укрепления экономической безопасности организаций в экономическом и правовом аспекте; оценивать ущерб от угроз информационной безопасности. **Владеть**: навыками принимать экономически и финансово обоснованные организационно-управленческие решения в профессиональной деятельности и нести за них ответственность в целях укрепления экономической безопасности организаций в экономическом и правовом аспекте; навыками обеспечения локальной и сетевой информационной безопасности.
ОПК-5 Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	**Знать:** международное и российское законодательство в сфере защиты информации. **Уметь:** подписывать документы с использованием технологий электронной подписи; **Владеть:** навыками администрирования программных средств шифрования данных в целях укрепления экономической безопасности.
ПК-1 Способность использовать современные методы сбора, накопления, структурирования и анализа данных с использованием специализированных программных продуктов; формировать аналитические отчёты	**Знать**: современные методы сбора, накопления, структурирования и анализа данных с использованием специализированных программных продуктов; основные способы безопасного хранения данных; возможности современных платформ бухгалтерского учета и налогообложения; способы формирования аналитических отчётов в целях эффективности использования государственных ресурсов и государственных закупок. **Уметь:** использовать современные методы сбора, накопления, структурирования и анализа данных с использованием специализированных программных продуктов; администрировать политики локальной безопасности; вести учет хозяйственной деятельности организации в конфигурациях с использованием специализированных программных продуктов; формировать аналитические отчёты в целях эффективности использования государственных ресурсов и государственных закупок. **Владеть:** навыками использовать современные методы сбора, накопления, структурирования и анализа данных с использованием специализированных программных продуктов; программными средствами журналирования и анализа событий безопасности; навыками генерации аналитической и бухгалтерской отчетности с использованием современных платформенных решений; формировать аналитические отчёты в целях эффективности

	использования государственных ресурсов и государственных закупок.
ПК-4 Способность получать юридически значимую информацию и на ее основе осуществлять мероприятия, направленную на профилактику, предупреждение преступлений и иных правонарушений в интересах выявление угроз и рисков финансовой безопасности	**Знать**: юридически значимую информацию и на ее основе осуществлять мероприятия, направленную на профилактику, предупреждение преступлений и иных правонарушений в интересах выявление угроз и рисков финансовой безопасности государственных и коммерческих организаций; основные риски и угрозы финансовой и информационной безопасности. **Уметь:** анализировать значимую информацию и на ее основе осуществлять мероприятия, направленную на профилактику, предупреждение преступлений и иных правонарушений в интересах выявление угроз и рисков финансовой безопасности государственных и коммерческих организаций; осуществлять мероприятия, направленные на профилактику преступлений и иных правонарушений в сфере финансовой и информационной безопасности на основе отчетности в специализированных программных продуктах. **Владеть:** навыками анализировать значимую информацию и на ее основе осуществлять мероприятия, направленную на профилактику, предупреждение преступлений и иных правонарушений в интересах выявление угроз и рисков финансовой безопасности государственных и коммерческих организаций; навыками оценивания ущерба от угроз финансовой и информационной безопасности.

3. Содержание дисциплины

Тема 1. Теоретические основы информационной безопасности.

Понятие информационной безопасности. Составляющие информационной безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Стандарт ISO/IEC 15408.

Тема 2. Технологии и протоколы защиты информации в IP-сетях.

Протоколы IPSec и трансляция сетевых адресов. Межсетевые экраны. Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.

Тема 3. Анализ и управление рисками в сфере информационной безопасности.

Модель безопасности с полным перекрытием. Управление информационной безопасностью. Методики построения систем защиты информации. Модель Lifecycle Security. Модель многоуровневой защиты. Методика управления рисками, предлагаемая MS.

4. Тематический план

№ п/п	Разделы и темы	Всего часов	Формы занятий			
			Лекции	Практич. занятия	Лаборатор. занятия	Самостоятельная работа
1.	Теоретические основы информационной безопасности	57	1	0	0	56
2.	Технологии и протоколы защиты информации в IP-сетях	59	1	0	2	56
3.	Анализ и управление рисками в сфере информационной безопасности	60	2	0	4	54
4.	Подготовка к зачету	4	0	0	0	4
Всего за семестр		180	4	0	6	170

5. Виды образовательной деятельности

Занятия лекционного типа

Лекция 1. (1 час)

Понятие информационной безопасности. Составляющие информационной безопасности. Общая схема процесса обеспечения безопасности. Уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ.

Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа.

Модели безопасности. Процесс построения и оценки системы обеспечения безопасности. Концепции стандарта ISO/IEC 15408.

Лекция 2. (1 час)

Сетевые протоколы IPSec и трансляция сетевых адресов. Технологии создания межсетевых экранов при передаче данных.

Лекция 3. (2 часа)

Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей.

Модель безопасности с полным перекрытием. Управление информационной безопасностью.

Методики построения систем защиты информации. Модель Lifecycle Security.

Модель многоуровневой защиты. Методика управления рисками, предлагаемая MS.

Занятия семинарского типа (лабораторные занятия)

Задания к лабораторным работам с подробными методическими рекомендациями и дополнительные материалы к лабораторным занятиям представлены в виде информационного контента на образовательном сервере **http://cdo.smolgu.ru**.

Лабораторная работа №1. Настройка политики безопасности и управление доступом к объектам файловой системы (**2 часа).** Цель работы: приобретение практических навыков по настройке разрешений на доступ к файлам в операционных системах семействах Windows.

Задание 1.

Произведите настройки приложения Проводник для эффективной работы с NTFS.

Определите права доступа пользователей к объектам диска.

Создайте папку с именем, соответствующим Вашей фамилии, на диске С. Для данной папки установите права доступа таким образом, чтобы только пользователь Student имел возможность просматривать и редактировать объекты папки.

Создайте нового пользователя системы с именем «ЛР» (Пуск – Панель управления – Учётные записи пользователей). Установите пароль для пользователя: 2.

Авторизуйтесь в системе от имени пользователя «ЛР». Попробуйте получить доступ к папке с именем, соответствующим Вашей фамилии, на диске С.

Авторизуйтесь в системе от имени пользователя «Студент». Для папки с именем, соответствующим Вашей фамилии, в Моих документах установите права доступа таким образом, чтобы все пользователи имели возможность просматривать и редактировать объекты папки.

Авторизуйтесь в системе от имени пользователя «ЛР». Попробуйте получить доступ к папке с именем, соответствующим Вашей фамилии, в Моих документах.

Авторизуйтесь в системе от имени пользователя «Студент». Удалите пользователя «ЛР» из системы.

Задание 2 (*для самостоятельного выполнения*).

Изучите управление политиками аудита безопасности в системе Windows. Управление политиками аудита можно осуществлять через оснастку «Локальные параметры безопасности». Для вызова оснастки «Локальные параметры безопасности» нажмите Пуск - Выполнить, наберите secpol.msc и нажмите ОК. Далее выберите «Локальные политики» - «Политика аудита».

Изучите аудит событий Windows и объектов файловой системы. После выбора политики аудита, изучение процесса аудита следует осуществлять экспериментальным путем в два этапа:

- выполнение действия, подлежащего аудиту (например, добавление новой учетной записи при включенной политике «Аудита управления учетными записями»);
- просмотр зарегистрированного события в журнале безопасности Windows.

При включении соответствующей политики аудита, регистрация событий аудита начинается автоматически. Это справедливо для всех политик аудита, кроме «Политики аудита доступа к объектам».

Для просмотра и управления журналом безопасности Windows используют оснастку «Просмотр событий». Для вызова оснастки необходимо: нажать Пуск > Выполнить и набрать eventvwr.msc и нажать ОК

Лабораторная работа №2. Сбор данных об информационной системе с помощью средств администрирования Windows и выявление уязвимостей системы **(2 часа).** Цель работы: приобретение навыков по сбору и анализу данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий сетевой доступ файловых ресурсах.

Задание 1.

Получите перечень компьютеров локальной сети. Для своего и соседнего компьютеров определите: Имя компьютера, IP-адрес и MAC-адрес.

Получите перечень предоставляемых в общий доступ ресурсов на вашем компьютере и на компьютере. Опишите хранимые там данные и охарактеризуйте степень их полезности и конфиденциальности.

Для указанных ресурсов и опишите действующие разрешения на доступ. При этом надо учитывать, что:

- эффективное (действующее) разрешение складывается из разрешений для пользователя лично и разрешений всех групп, в которые пользователь входит;
- запрещение имеет больший приоритет, чем разрешение;
- при комбинации разрешений для общего ресурса с разрешениями NTFS, приоритетными будут разрешения, максимально ограничивающие доступ.

Перечислите все активные сетевые соединения на своём компьютере с информацией об именах исполняемых файлов.

Определите DNS СДО СмолГУ. Постройте маршрут пакетов от Вашего компьютера до СДО СмолГУ.

Задание 2 (*для самостоятельного выполнения*).

С помощью утилиты NetView просканировать локальную сеть, определить IP, MAC, ресурсы общего доступа, учётные записи пользователей своего и соседнего компьютера.

Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. Укажите:

– как оценен уровень уязвимости Вашего компьютера;

– какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;

– опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

Проведите анализ результатов. Какие уязвимости можно устранить, какие – нельзя из-за особенностей конфигурации ПО или использования компьютера?

Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.

Опишите действующую на вашем компьютере политику паролей. Если в ходе проверки утилитой BSA были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

Лабораторная работа №3. Анализ и управление рисками **(2 часа).** Цель работы: приобретение практических навыков по выявлению рисков в информационных системах и управлению настроек программных средств по их снижению.

Задание 1.

Проведите сканирование своего и соседнего компьютеров в учебной лаборатории. При сканировании надо учитывать, что часть имеющихся уязвимостей может быть закрыта путем использования встроенного межсетевого экрана (брандмауэра Windows). Чтобы получить более полную информацию об исследуемых узлах, лучше провести одно сканирование при включенном, другое - при отключенном межсетевом экране (изменение настройки доступно через Панель управления -> Брандмауэр Windows). Аналогичная ситуация возникает и при использовании других межсетевых экранов.

Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров. При анализе результатов сканирования используйте техническую статью «Службы и сетевые порты в серверных системах Microsoft Windows», доступную по ссылке http://support.microsoft.com/?kbid=832017.

Проведите сканирование домена smolgu.ru. Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров. При анализе результатов сканирования используйте техническую статью «Службы и сетевые порты в серверных системах Microsoft Windows», доступную по ссылке http://support.microsoft.com/?kbid=832017.

Просканируйте Ваш компьютер с помощью сервисов сканирования настроек безопасности и опишите результаты проверки:

http://portscan.ru/portscanner.html
http://www.testip.ru/services/portscan.html
https://2ip.ru/port-scaner/

Задание 2.

Составьте бизнес-модель компании, которая активно использует компьютерную технику, сетевое оборудование, информационные технологии и системы в своей деятельности. Уделите особое внимание мерам по обеспечению информационной безопасности на предприятии и расходам на их реализацию.

Подробно опишите реально существующее или вымышленное малое предприятие (до 1000 сотрудников): сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства и т.д.

С помощью программы MSAT проведите оценку рисков для предприятия. Сформируйте и сохраните полный и расширенный отчеты MSAT.

Задание 3 (*для самостоятельного выполнения*)

Просмотрите параметры сертификата «Сбербанк Онлайн» Сбербанка – https://online.sberbank.ru/CSAFront/index.do. Сделайте скриншот, опишите, кем, на какой срок и для какого субъекта сертификат был выдан.

Выявите процесс хранения сертификатов в ОС Windows. Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку консоль управления MMC «Сертификаты».

Из меню Пуск -> Выполнить запустите консоль командой mmc. В меню Консоль выберите Добавить или удалить оснастку, а в списке оснасток выберите Сертификаты. Если будет предложен выбор (а это произойдет, если Вы работаете с правами администратора), выберите пункт «Моей учетной записи».

В разделе «Доверенные корневые центры сертификации» представлен достаточно обширный список центров, чьи сертификаты поставляются вместе с операционной системой.

Найдите в нем сертификат VeriSign Class 3 Public Primary CA. Благодаря тому, что он уже был установлен, в рассмотренном в начале работы примере с подключением к системам Интернет-банкинга браузер мог подтвердить подлинность узла.

Самостоятельная работа

Задания для самостоятельного выполнения разбиты в соответствии с тематическим планированием курса и являются гармоничным дополнением к лабораторным работам (см. пункт «Виды учебной деятельности. Лабораторные занятия»).

Вопросы для самостоятельного изучения по дисциплине

Тема 1.

1. В чем заключается проблема «информационной безопасности»?
2. Дайте определение «информационной безопасности».
3. Перечислите составляющие информационной безопасности и их определение.

4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.

5. Перечислите уровни формирования режима информационной безопасности.

6. Перечислите основополагающие документы по «информационной безопасности».

7. Основные задачи «информационной безопасности» в соответствии с Концепцией национальной безопасности РФ.

8. Какие виды требований включает стандарт ISO/IEC 15408?

9. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.

10. Перечислите основные механизмы безопасности.

11. Что понимается под администрированием средств безопасности?

12. Классы защищенности межсетевых экранов.

13. Содержание административного уровня обеспечения «информационной безопасности».

14. На чем основан механизм регистрации?

15. Какие события, связанные с безопасностью, подлежат регистрации?

16. Чем отличаются механизмы регистрации и аудита?

17. Какие этапы предусматривают механизмы регистрации и аудита?

18. Дайте определение политики безопасности.

19. Направления разработки политики безопасности.

20. Перечислите классы угроз информационной безопасности.

21. Назовите причины и источники случайных воздействий на информационные системы.

22. Дайте характеристику преднамеренным угрозам.

23. Перечислите каналы несанкционированного доступа.

24. Что понимается под техническим каналом утечки информации?

25. Каковы причины возникновения электромагнитных каналов утечки информации?

26. Как образуется параметрический канал утечки информации?

27. Основные угрозы целостности информации.

28. Охарактеризуйте угрозы доступности информации.

Тема 2.

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды «вирусоподобных» программ.
9. Поясните механизм функционирования «троянской программы» (логической бомбы).
10. Поясните понятия «сканирование на лету» и «сканирование по запросу».
11. Перечислите виды антивирусных программ.
12. Охарактеризуйте антивирусные сканеры.
13. В чем особенности эвристических сканеров?
14. Какие факторы определяют качество антивирусной программы?
15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.

16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
17. Характерные черты макровируса.
18. Как проверить систему на наличие макровируса?
19. В чем заключаются особенности обеспечения «информационной безопасности» компьютерных сетей?
20. Дайте определение понятия «удаленная угроза».
21. В чем заключается специфика методов и средств защиты компьютерных сетей?
22. Поясните понятие «глобальная сетевая атака», приведите примеры.
23. Какие протоколы образуют модель TCP/IP?
24. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?
25. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.
26. На каком уровне модели OSI/ISO реализуется сервис безопасности «неотказуемость» (согласно «Общим критериям»)?
27. Для чего предназначен DNS-сервер?
28. Перечислите классы удаленных угроз.
29. Как классифицируются удаленные угрозы «по характеру воздействия»?
30. Охарактеризуйте удаленные угрозы «по цели воздействия».
31. Может ли пассивная угроза привести к нарушению целостности информации?
32. Дайте определение типовой удаленной атаки.
33. Что является целью злоумышленников при «анализе сетевого трафика»?
34. Назовите причины успеха удаленной атаки «ложный объект».

Тема 3.

1. Что понимается под идентификацией и аутентификацией пользователя?
2. Перечислите возможные идентификаторы при реализации механизмов идентификации и аутентификации.
3. Что такое «электронный ключ»?
4. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
5. Что входит в состав криптосистемы?
6. Как реализуются симметричный и асимметричный методы шифрования?
7. Что такое электронная цифровая подпись?
8. Перечислите методы разграничения доступа.
9. Какие методы управления доступом предусмотрены в руководящих документах Гостехкомиссии?
10. В чем заключается принцип межсетевого экранирования?
11. Принцип функционирования межсетевых экранов с фильтрацией пакетов.
12. Какие сервисы безопасности включает технология виртуальных частных сетей?
13. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
14. Чем определяется политика безопасности виртуальной частной сети?

6. Критерии оценивания результатов освоения дисциплины (модуля)

6.1. Оценочные средства и критерии оценивания для текущей аттестации

Вопросы для самостоятельного изучения

Тема 1.

1. В чем заключается проблема «информационной безопасности»?
2. Дайте определение «информационной безопасности».
3. Перечислите составляющие информационной безопасности и их определение.
4. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
5. Перечислите уровни формирования режима информационной безопасности.
6. Перечислите основополагающие документы по «информационной безопасности».
7. Основные задачи «информационной безопасности» в соответствии с Концепцией национальной безопасности РФ.
8. Какие виды требований включает стандарт ISO/IEC 15408?
9. Дайте характеристику составляющих «информационной безопасности» применительно к вычислительным сетям.
10. Перечислите основные механизмы безопасности.
11. Что понимается под администрированием средств безопасности?
12. Классы защищенности межсетевых экранов.
13. Содержание административного уровня обеспечения «информационной безопасности».
14. На чем основан механизм регистрации?
15. Какие события, связанные с безопасностью, подлежат регистрации?
16. Чем отличаются механизмы регистрации и аудита?
17. Какие этапы предусматривают механизмы регистрации и аудита?
18. Дайте определение политики безопасности.
19. Направления разработки политики безопасности.
20. Перечислите классы угроз информационной безопасности.
21. Назовите причины и источники случайных воздействий на информационные системы.
22. Дайте характеристику преднамеренным угрозам.
23. Перечислите каналы несанкционированного доступа.
24. Что понимается под техническим каналом утечки информации?
25. Каковы причины возникновения электромагнитных каналов утечки информации?
26. Как образуется параметрический канал утечки информации?
27. Основные угрозы целостности информации.
28. Охарактеризуйте угрозы доступности информации.

Тема 2.

1. Каковы характерные черты компьютерных вирусов?
2. Дайте определение программного вируса.
3. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
4. Перечислите классификационные признаки компьютерных вирусов.
5. В чем особенности резидентных вирусов?
6. Перечислите деструктивные возможности компьютерных вирусов.
7. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
8. Перечислите виды «вирусоподобных» программ.
9. Поясните механизм функционирования «троянской программы» (логической бомбы).
10. Поясните понятия «сканирование на лету» и «сканирование по запросу».
11. Перечислите виды антивирусных программ.
12. Охарактеризуйте антивирусные сканеры.
13. В чем особенности эвристических сканеров?
14. Какие факторы определяют качество антивирусной программы?

15. Перечислите наиболее распространенные пути заражения компьютеров вирусами.

16. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.

17. Характерные черты макровируса.

18. Как проверить систему на наличие макровируса?

19. В чем заключаются особенности обеспечения «информационной безопасности» компьютерных сетей?

20. Дайте определение понятия «удаленная угроза».

21. В чем заключается специфика методов и средств защиты компьютерных сетей?

22. Поясните понятие «глобальная сетевая атака», приведите примеры.

23. Какие протоколы образуют модель TCP/IP?

24. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?

25. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.

26. На каком уровне модели OSI/ISO реализуется сервис безопасности «неотказуемость» (согласно «Общим критериям»)?

27. Для чего предназначен DNS-сервер?

28. Перечислите классы удаленных угроз.

29. Как классифицируются удаленные угрозы «по характеру воздействия»?

30. Охарактеризуйте удаленные угрозы «по цели воздействия».

31. Может ли пассивная угроза привести к нарушению целостности информации?

32. Дайте определение типовой удаленной атаки.

33. Что является целью злоумышленников при «анализе сетевого трафика»?

34. Назовите причины успеха удаленной атаки «ложный объект».

Тема 3.

1. Что понимается под идентификацией и аутентификацией пользователя?

2. Перечислите возможные идентификаторы при реализации механизмов идентификации и аутентификации.

3. Что такое «электронный ключ»?

4. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?

5. Что входит в состав криптосистемы?

6. Как реализуются симметричный и асимметричный методы шифрования?

7. Что такое электронная цифровая подпись?

8. Перечислите методы разграничения доступа.

9. Какие методы управления доступом предусмотрены в руководящих документах Гостехкомиссии?

10. В чем заключается принцип межсетевого экранирования?

11. Принцип функционирования межсетевых экранов с фильтрацией пакетов.

12. Какие сервисы безопасности включает технология виртуальных частных сетей?

13. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?

14. Чем определяется политика безопасности виртуальной частной сети?

Критерии оценивания ответов на вопросы для самостоятельного изучения

Ответ по каждому вопросу оценивается по пятибалльной шкале в зависимости от содержательности ответа и логики изложения материала.

Уровень ответа	**Оценка**

Полно и аргументировано отвечает по содержанию темы; может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из лекции, но и самостоятельно составленные; излагает материал последовательно и корректно.	5 (отлично)
Дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1-2 ошибки, которые сам же исправляет.	4 (хорошо)
Излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки.	3 (удовлетворительно)
Не знает ответ на вопрос, допускает существенные ошибки в формулировке определений и алгоритмов, искажающие их смысл, беспорядочно и неуверенно излагает материал.	2 (неудовлетворительно)

Задания для самостоятельного выполнения

Задания для самостоятельного выполнения разбиты в соответствии с тематическим планированием курса и являются гармоничным дополнением к лабораторным работам.

Задание для самостоятельного выполнения 1.

Изучите управление политиками аудита безопасности в системе Windows. Управление политиками аудита можно осуществлять через оснастку «Локальные параметры безопасности». Для вызова оснастки «Локальные параметры безопасности» нажмите Пуск - Выполнить, наберите secpol.msc и нажмите ОК. Далее выберите «Локальные политики» - «Политика аудита».

Изучите аудит событий Windows и объектов файловой системы. После выбора политики аудита, изучение процесса аудита следует осуществлять экспериментальным путем в два этапа:

- выполнение действия, подлежащего аудиту (например, добавление новой учетной записи при включенной политике «Аудита управления учетными записями»);
- просмотр зарегистрированного события в журнале безопасности Windows.

При включении соответствующей политики аудита, регистрация событий аудита начинается автоматически. Это справедливо для всех политик аудита, кроме «Политики аудита доступа к объектам».

Для просмотра и управления журналом безопасности Windows используют оснастку «Просмотр событий». Для вызова оснастки необходимо: нажать Пуск > Выполнить и набрать eventvwr.msc и нажать ОК

Задание для самостоятельного выполнения 2.

С помощью утилиты NetView просканировать локальную сеть, определить IP, MAC, ресурсы общего доступа, учётные записи пользователей своего и соседнего компьютера.

Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. Укажите:

– как оценен уровень уязвимости Вашего компьютера;

– какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;

– опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

Проведите анализ результатов. Какие уязвимости можно устранить, какие – нельзя из-за особенностей конфигурации ПО или использования компьютера?

Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.

Опишите действующую на вашем компьютере политику паролей. Если в ходе проверки утилитой BSA были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

Задание для самостоятельного выполнения 3.

Просмотрите параметры сертификата «Сбербанк Онлайн» Сбербанка – https://online.sberbank.ru/CSAFront/index.do. Сделайте скриншот, опишите, кем, на какой срок и для какого субъекта сертификат был выдан.

Выявите процесс хранения сертификатов в ОС Windows. Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку консоль управления MMC «Сертификаты».

Из меню Пуск -> Выполнить запустите консоль командой mmc. В меню Консоль выберите Добавить или удалить оснастку, а в списке оснасток выберите Сертификаты. Если будет предложен выбор (а это произойдет, если Вы работаете с правами администратора), выберите пункт «Моей учетной записи».

В разделе «Доверенные корневые центры сертификации» представлен достаточно обширный список центров, чьи сертификаты поставляются вместе с операционной системой.

Найдите в нем сертификат VeriSign Class 3 Public Primary CA. Благодаря тому, что он уже был установлен, в рассмотренном в начале работы примере с подключением к системам Интернет-банкинга браузер мог подтвердить подлинность узла.

Критерии оценивания заданий для самостоятельного выполнения.

Уровень выполнения	Оценка
Задача решена в полном объёме, алгоритмические и вычислительные ошибки отсутствуют, проведен анализ полученного решения.	5 (отлично)
Задача решена в полном объёме с незначительными техническими ошибками или отсутствует анализ результатов решения.	4 (хорошо)
Задача решена не полностью или в решении присутствуют ошибки алгоритмического характера, незначительно влияющие на ход решения.	3 (удовлетворительно)
Задача не решена или в решении присутствует значительное количество ошибок алгоритмического характера, существенно влияющих на ход решения.	2 (неудовлетворительно)

6.2. Оценочные средства и критерии оценивания для промежуточной аттестации

Критерии получения зачета

Зачет выставляется по результатам работы студента в течение семестра согласно Положению о текущем контроле успеваемости и промежуточной аттестации студентов в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Смоленский государственный университет».

Для получения зачета студент должен:

- выполнить задания лабораторных работ на оценку не ниже «удовлетворительно»;
- выполнить задания для самостоятельной работы на оценку не ниже «удовлетворительно»;
- уметь отвечать на вопросы для самостоятельного изучения на оценку не ниже «удовлетворительно».

7. Перечень основной и дополнительной учебной литературы

7.1. Основная литература

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/444046
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/433715
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/432966
4. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/477968
5. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370
6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

7.2. Дополнительная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/432966

2. Галатенко В. Основы информационной безопасности. Национальный открытый университет ИНТУИТ. URL: https://www.intuit.ru/studies/courses/10/10/info (дата обращения 10.10.2019).
3. Граничин О., Князев В. Безопасность информационных систем. Национальный открытый университет ИНТУИТ. URL: https://www.intuit.ru/studies/courses/13845/1242/info

7.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Свободно доступные курсы Интернет-университета информационных технологий (ИНТУИТ) http://www.intuit.ru/;

2. Портал государственных и муниципальных услуг. http://www.gosuslugi.ru/;

3. Официальный сайт ЗАО «Консультант Плюс» – www.consultant.ru;

4. Официальный сайт ООО «НПП Гарант-Сервис» – www.garant.ru;

Методические указания для обучающихся по освоению дисциплины

1. Мультимедийные презентации PowerPoint для проведения лекций.
2. Комплексы лабораторных работ, представленные в виде информационного контента.

Электронные материалы размещены на образовательном сервере СмолГУ **http://cdo.smolgu.ru**.

8. Материально-техническое обеспечение

Учебная аудитория для проведения занятий лекционного типа. Аудитория 124 уч.к. № 2.

Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.

Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.

Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – компьютерный класс. Аудитория 124 уч.к. №2.

Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.

Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 16 шт., колонки Genius – 16 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.

Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

Помещение для самостоятельной работы – компьютерный класс с доступом к сети «Интернет» и ЭИОС СмолГУ. Аудитория 124 уч.к. №2.

Стандартная учебная мебель (40 учебных посадочных мест), стол и стул для преподавателя – по 1 шт., кафедра для лектора – 1 шт.

Компьютерные студенческие столы (17 шт.), компьютерный стол для преподавателя – 1 шт., мониторы Acer – 18 шт., системные блоки Kraftway – 18 шт., колонки Genius – 18 шт., мультимедиапроектор BenQ – 1 шт., интерактивная доска Interwrite – 1 шт. Обеспечен выход в Интернет.

Программное обеспечение: Microsoft Open License (Windows XP, 7, 8, 10, Server, Office 2003-2016), лицензия 66975477 от 03.06.2016 (бессрочно).

9. Программное обеспечение

1. Microsoft Open License, лицензия 49463448 в составе:
   – Microsoft Windows Professional 10 Russian;
   – Microsoft Office 2016 Russian.
2. СКЗИ КриптоПро (лицензия, интегрированная в сертификат для образовательных курсов в рамках программы академического партнерства с СКБ Контур).
3. Веб-сервисы безбумажного юридически значимого документооборота компании СКБ «Контур» (в рамках программы академического партнерства с СКБ Контур).